NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

ASSESSING AND MINIMIZING ADVERSARIAL RISK IN A NUCLEAR MATERIAL TRANSPORTATION NETWORK

by

Bradford S. Foster

September 2013

Thesis Advisor:	R. Kevin Wood
Second Reader:	Kyle Y. Lin

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*

2. REPORT DATE
09-27-2013

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE

ASSESSING AND MINIMIZING ADVERSARIAL RISK IN A NUCLEAR MATERIAL TRANSPORTATION NETWORK

5. FUNDING NUMBERS

6. AUTHOR(S)

Bradford S. Foster

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Postgraduate School
Monterey, CA 93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Department of the Navy

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol Number: N/A

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

This thesis develops a simple method for evaluating adversarial risk within the transportation portion of the nuclear fuel cycle for commercial electric power generation, and develops models that can guide the reduction of that risk by such means as rerouting and decoy shipments. A conceivable, worst-case attack by an intelligent adversary will cause a localized release of radioactive material. A damage function is defined using the population in the vicinity of the attack. Using hypothetical, but realistic, transit routes between fuel fabricators and power plants, we identify the worst-case locations for attack. Then we formulate and solve mixed-integer programs to either (a) redesign the network by changing supply contracts, or (b) optimally allocate a resource-constrained assignment of decoy shipments. We also demonstrate a greedy procedure for simple rerouting of individual shipments. Computational methods exploit standard geographical databases, and optimization software solves the models in seconds on a personal computer. Separate but similar analyses would apply to shipments of uranium hexafluoride, spent fuel being shipped for reprocessing, spent fuel being shipped to a repository, and other materials.

14. SUBJECT TERMS

Nuclear material, Hazmat, Transportation network, Adversarial risk, Mixed integer programming, Decoy

15. NUMBER OF PAGES 67

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

ASSESSING AND MINIMIZING ADVERSARIAL RISK IN A NUCLEAR MATERIAL TRANSPORTATION NETWORK

Bradford S. Foster
Lieutenant, United States Navy
B.S., Texas A&M University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author:	Bradford S. Foster
Approved by:	R. Kevin Wood Thesis Advisor
	Kyle Y. Lin Second Reader
	Robert F. Dell Chair, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis develops a simple method for evaluating adversarial risk within the transportation portion of the nuclear fuel cycle for commercial electric power generation, and develops models that can guide the reduction of that risk by such means as rerouting and decoy shipments. A conceivable, worst-case attack by an intelligent adversary will cause a localized release of radioactive material. A damage function is defined using the population in the vicinity of the attack. Using hypothetical, but realistic, transit routes between fuel fabricators and power plants, we identify the worst-case locations for attack. Then we formulate and solve mixed-integer programs to either (a) redesign the network by changing supply contracts, or (b) optimally allocate a resource-constrained assignment of decoy shipments. We also demonstrate a greedy procedure for simple rerouting of individual shipments. Computational methods exploit standard geographical databases, and optimization software solves the models in seconds on a personal computer. Separate but similar analyses would apply to shipments of uranium hexafluoride, spent fuel being shipped for reprocessing, spent fuel being shipped to a repository, and other materials.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

1 INTRODUCTION **1**

2 BACKGROUND: TRANSPORTATION IN THE NUCLEAR FUEL CYCLE **3**

3 DEFINING ADVERSARIAL RISK **7**

3.1 A Basic Model of Risk 7

3.2 Other Models of Adversarial Risk. 10

4 SUBNETWORKS IN THE DOMESTIC NUCLEAR FUEL CYCLE **13**

5 EVALUATING ADVERSARIAL RISK OR ITS SURROGATE FOR A SUBNETWORK **15**

5.1 Damage Values for a "Direct Attack" 15

5.2 Damage Values for a "Hijacking Attack" 18

5.3 Reducing Adversarial Risk 19

6 DA1: A GENERAL DEFENDER-ATTACKER MODEL FOR REDUCING ADVERSARIAL RISK IN A TRANSPORTATION SUBNETWORK **21**

6.1 A General Model: DA1 21

6.2 An Application of DA1: Recontracting. 24

6.3 Simple Rerouting: A Greedy Approach 26

7 DA2: REDUCING EXPECTED RISK WITH DECOY SHIPMENTS **29**

7.1 Allocating Decoys Optimally: DA2 29

7.2 A Sample Application of Decoys 30

8 CONCLUSIONS **33**

Appendix: Realistic Test Data **35**

References **42**

Initial Distribution List **46**

List of Figures

Figure 2.1 Transportation in the nuclear fuel cycle. Solid dark arrows represent movement of nuclear material between facilities in the current U.S. fuel cycle; the light-shaded solid arrow shows a movement that could involve transportation in a non-U.S. cycle. Dashed arrows represent potential transportation of nuclear material in future fuel cycles. Many shipments of spent fuel have occurred in the U.S., but these have been on an ad hoc basis (e.g., to consolidate storage for a single power producer). These shipments have not been part of an operating fuel cycle [4], as they have been in other countries. . . 4

Figure 2.2 U.S. facilities that process nuclear materials at various stages of the nuclear fuel cycle. 5

Figure 2.3 Commercial nuclear power reactors operating in the U.S. as of July 2013. 6

Figure A.1 Google Earth routing from Areva to Arkansas Nuclear One as it transits Colorado, shown as a heavy black line. 38

Figure A.2 Colorado hazardous and nuclear materials route restrictions. Approved nuclear materials routes are shown in green. A shipment from Areva to Arkansas Nuclear One might take the route that is highlighted in black over the approved nuclear materials routes on I-25 and I-70. Along with Figure A.1, this demonstrates that the "fastest-path" routing from Google gives a partial route that is plausible given HAZMAT road restrictions. After [34]. 39

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

Table 5.1 The 10 largest damage values and their locations given (a) a direct attack, and (b) the affected population resides in only a single population cell. The related number of affected routes and reactors is also given. For example, nine routes traverse a single location near Chicago, Illinois, where the population data imply a damage value of 261787; those nine routes feed 15 reactors. 17

Table 5.2 The 10 largest damage values for an attack that occurs in a given cell and affects that cell along with the eight adjacent cells. See the caption for Table 5.1 for additional information. 17

Table 5.3 For a hijacking attack, the 10 largest damage values and their locations. A shipment hijacked on the hypothetical route from Westinghouse to Braidwood is farther than 30 miles from the peak population area of Chicago, Illinois, and a hijacked truck could only reach the suburbs to the south of the Chicago under assumed conditions. . . 19

Table 6.1 Routes with the largest damage values. For example, nine routes traverse the same road segment near Chicago, Illinois, which imposes the largest damage value of any location on any route. 25

Table 6.2 Largest damage values after recontracting. 25

Table 6.3 Recontracting. Thirteen nuclear fuel supply contracts change. Additional changes to business contracts do not lower the overall risk for the network. While avoiding Chicago, the worst-case damage of 225895 occurs for shipments traveling on I-95 past Newark, New Jersey. 26

Table 6.4 These routes all define the maximum damage value of 261787 in the baseline (“initial”) system. To reduce overall risk by rerouting, all nine routes through Chicago must be modified in some way. We restrict rerouting decisions to use I-74 through Champaign, Illinois. The Millstone-Areva route now defines risk for this subnetwork because its damage value of 220173 is greatest. 27

Table 7.1 Optimal reductions in expected damage as total decoy-miles increase. 31

Table A.1 Partly hypothetical fuel-fabricator-to-power-plant assignments, with number of reactors at each power plant. These assignments define the baseline fresh-fuel subnetwork in computational tests. 37

List of Acronyms and Abbreviations

AVLIS	atomic vapor laser isotope separation
DA	defender-attacker
DAD	defender-attacker-defender
DoE	Department of Energy
GNF	Global Nuclear Fuel – Americas, LLC
HAZMAT	hazardous material
kg	kilogram
km	kilometer
LWR	light water reactor
MWt	megawatt thermal
MOX	mixed-oxide fuel
MTW	Honeywell Metropolis Works
PRA	probabilistic risk analysis
RIMES	Risk-Informed Management of Enterprise Security
SILEX	separation of isotopes by laser excitation
SME	subject matter expert
TVA	Tennessee Valley Authority
USEC	United States Enrichment Corporation

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

This thesis develops a simple method for evaluating *adversarial risk* within the transportation portion of the nuclear fuel cycle for commercial electric power generation, and develops models that can guide the reduction of that risk by such means as rerouting and decoy shipments. The research focuses on the U.S. fuel cycle, but the methods developed are flexible enough to handle current and future fuel cycles around the world. "Adversarial risk" measures the potential danger posed by an intelligent adversary who might (a) attack a shipment and steal material to to be used in an improvised nuclear device, or (b) attack a shipment with one or more explosive devices and cause a direct release of dangerous materials into the environment, or (c) hijack a shipment, move it to a new location, and then release some of the contents into the environment.

"Adversarial" covers conceivable, worst-case attacks by an intelligent adversary. Stealing dangerous material from a shipment is almost inconceivable given the safeguards in shipping and the great bulk of the containers used for shipping uranium hexafluoride, fresh nuclear fuel, and spent nuclear fuel. Therefore, we do not consider case (a). Furthermore, we do not view the theft of yellowcake as a serious threat since it must undergo a complicated enrichment process before becoming dangerous. On the other hand, a literature review indicates that a terrorist organization, using weapons and methods that may lie within that organization's reach, could strike a shipment of nuclear material successfully; enough material could be released to inflict substantial physical and economic damage. A hijacking attack appears much less likely to succeed, but our methods extend to analyze such scenarios.

Both rail and truck shipments are subject to adversarial risks. We limit most discussion and development to truck shipments, however, because the thesis's methods carry over from truck to rail shipments in a straightforward fashion.

Focusing on directs attacks (b), we note that any existing "damage function" for a worst-case attack will yield monotonically increasing values as a function of the total population affected, namely, the population in a model-defined area surrounding a shipping route. This monotonicity allows us to use population in an area around a point on a transportation

route as a surrogate for the “true damage” that would accrue from an attack at that point. The surrogate then generates the objective function for several game-theoretic models for minimizing adversarial risk or expected adversarial risk.

To illustrate, we use hypothetical but realistic data to evaluate adversarial risk for fresh-fuel shipments in the United States, and show how to (a) minimize adversarial risk by redesigning the network so that shipments travel through areas that would be “less risky,” or (b) minimize expected adversarial risk by a resource-constrained assignment of decoy shipments. “Redesign” in (a) could mean renegotiating supply contracts or simply rerouting individual shipments. Depending on problem specifics, optimization of these “defender-attacker models” is achieved by solving an integer program or by applying a simple greedy procedure. Separate but similar analyses would apply to shipments of uranium hexafluoride, spent fuel being shipped for reprocessing, spent fuel being shipped to a repository, and other materials.

Because a simple surrogate risk measure applies for adversarial risk analysis, data requirements are modest. Furthermore, computational methods exploit standard geographical databases and optimization software. Again focusing on fresh-fuel transportation, computations provide results of the following form:

1. Under reasonable constraints, renegotiation of fuel supplies (i.e., supplier-to-power-plant assignments) could reduce the risk surrogate by $g\%$. Furthermore, a linear relationship between the surrogate and actual damage might be reasonably assumed, so actual risk might be reduced by $g\%$, also.
2. Without rerouting, expected risk for fresh-fuel shipments can be reduced by $h\%$ through the use of decoy shipments with a total mileage limit of m miles per year.

Acknowledgements

I would like to thank my advisor, Professor Kevin Wood, for the tremendous amount of help he provided in seeing this thesis through to completion. I would also like to thank Professor Kyle Lin, Professor David Alderson, and Professor Nedialko Dimitrov for their input throughout the whole process.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 1: INTRODUCTION

The U.S. Department of Energy (DoE) and others are concerned with the risk of “damage” from an attack on the transportation portion of a commercial nuclear fuel cycle, domestic or foreign [1]. This thesis develops and demonstrates a general model for (a) evaluating this “adversarial risk” and (b) minimizing this risk subject to resource constraints.

An attack could involve the destruction of a shipment of feedstock and the exposure of a local population to a toxic and/or radioactive substance, or it could involve the theft of material that would be converted into a fission or nuclear-dispersion weapon, and then unleashed upon a population. Damage might involve only bad publicity, although this could have a substantial economic effect on the industry. But, the possibility exists that damage would mean the loss of thousands of lives from the explosion of, say, a nuclear-dispersion device.

This thesis creates a surrogate model for evaluating adversarial risk and applies that to create the objective function for several new game-theoretic risk-reduction models. Using realistic but notional data, we demonstrate with several examples. For example, given that “risk of damage” from an attack on a given shipment increases monotonically with the population that might be affected, we show how a cardinality-restricted set of origin-destination pairs might be modified to minimize risk.

The rest of this thesis proceeds as follows. Chapter 2 reviews the nuclear fuel cycle, with a focus on the transportation of nuclear material between facilities. Chapter 3 develops a general model for evaluating adversarial risk in this context. Chapter 4 describes the transportation “subnetworks” that may be analyzed individually for adversarial risk, for example, the subnetwork that ships fresh-fuel assemblies. Then, using realistic but notional data, Chapter 5 demonstrates use of the adversarial-risk model by analyzing the “fresh-fuel subnetwork.” Chapter 6 describes a generic, game-theoretic, defender-attacker model, which seeks to design a minimum-risk subnetwork subject to resource constraints. This extends to modifying existing networks to minimize risk, which is demonstrated for the fresh-fuel network. Chapter 7 describes a general optimization model for assigning decoy shipments to reduce expected adversarial risk; again the fresh-fuel subnetwork is used to demonstrate. Finally, an appendix describes how we collect and manipulate real and notional data for model-demonstration purposes.

CHAPTER 2: BACKGROUND: TRANSPORTATION IN THE NUCLEAR FUEL CYCLE

This chapter explains the transportation portion of a commercial nuclear fuel cycle, with a focus on the U.S. This provides important background for developing and demonstrating a useful model of adversarial risk.

In its simplest form, the nuclear fuel cycle in the U.S. consists of several stages for preparing, consuming, and disposing of nuclear material. Figure 2.1 depicts the basic processing steps in current and future fuel cycles, and the flow of material between these steps. Each of the steps requires specialized equipment, often located in standalone facilities. Thus, nuclear materials must be transported between facilities to proceed through some processing steps. Focusing on transportation, we can understand the overall nuclear fuel cycle as a supply chain that transports material from its "raw" form to "finished product" to "waste."

1. *Mining and Milling.* Uranium ore is mined or removed from the earth in a leaching process.
2. *Conversion (1).* Triuranium octoxide (U_3O_8, "yellowcake") is converted into uranium hexafluoride (UF_6) for subsequent enrichment.
3. *Enrichment.* UF_6 is processed, removing ^{238}U to to increase the percentage of fissile ^{235}U. This process typically involves a gaseous centrifuge, but a number of techniques are known, such as the "separation of isotopes by laser excitation" (SILEX) process, which has been licensed recently [2].
   Note: Public information on the SILEX process indicates that it uses UF_6 as a feedstock. Thus, the overall physical structure of the supply chain may not change under SILEX enrichment. This may not be true with the earlier "atomic vapor laser isotope separation" (AVLIS) process, which may still be viable, at least outside the U.S. This process uses vaporized uranium as feedstock [3].
4. *Conversion (2).* Enriched UF_6 is converted into (enriched) uranium dioxide (UO_2), which is then fired into ceramic pellets for placement in fuel rods.

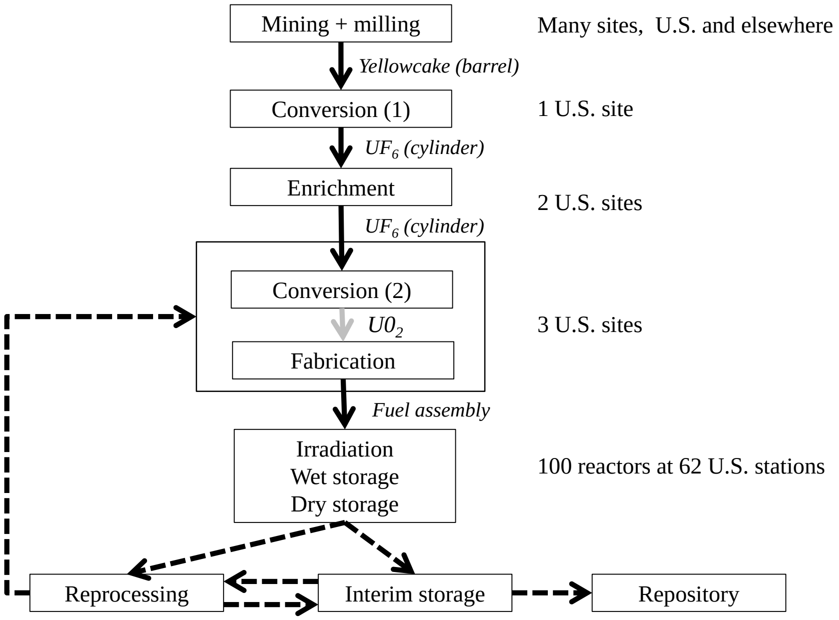

Figure 2.1: Transportation in the nuclear fuel cycle. Solid dark arrows represent movement of nuclear material between facilities in the current U.S. fuel cycle; the light-shaded solid arrow shows a movement that could involve transportation in a non-U.S. cycle. Dashed arrows represent potential transportation of nuclear material in future fuel cycles. Many shipments of spent fuel have occurred in the U.S., but these have been on an ad hoc basis (e.g., to consolidate storage for a single power producer). These shipments have not been part of an operating fuel cycle [4], as they have been in other countries.

5. *Fabrication.* Fuel rods are constructed from enriched uranium pellets, and gathered into the bundles that make up a fuel assembly, as used in power-plant reactors.
6. *Irradiation.* Complete fuel assemblies are installed in a power reactor, and controlled nuclear fission is initiated for the purpose of generating electric power.
7. *On-site storage.* Once a fuel assembly has reached the end of its useful life, it is removed and placed into on-site wet-waste storage. Here, it cools over many months until it can be dried and placed into semi-permanent dry-waste storage. Eventually, dry-waste must be sent to a permanent repository or recycled, but on-site dry storage is the current end of the U.S. nuclear fuel cycle.
8. *Reprocessing.* Spent fuel can be reprocessed to concentrate certain radioisotopes. This concentrated material would then be sent to conversion and fabrication facilities where it would become part of new fuel assemblies. Material from nuclear weapons

can be "reprocessed" in a similar fashion to provide reactor fuel.

9. *Interim storage.* It is possible that a non-permanent storage facility would be created to store dry waste from one or more nuclear power plants. This would allow power plants whose on-site storage has reached capacity to continue operating, even though no permanent repository had been built.
10. *Repository.* Waste material from an interim storage site or from a power plant's dry-waste storage would be transported to a permanent storage site (i.e., a repository). Yucca Mountain was intended to be such a repository [5].

Only a few facilities in the United States perform the processing steps described above. Figure 2.2 displays the locations of the processing facilities currently in the U.S. The ultimate consumers of nuclear fuel are reactor facilities that generate electricity. Figure 2.3 displays the locations and ages of the nuclear reactors currently operating in the U.S. Together, these figures should give the reader an idea of the geographical scope of the models we are pursuing.

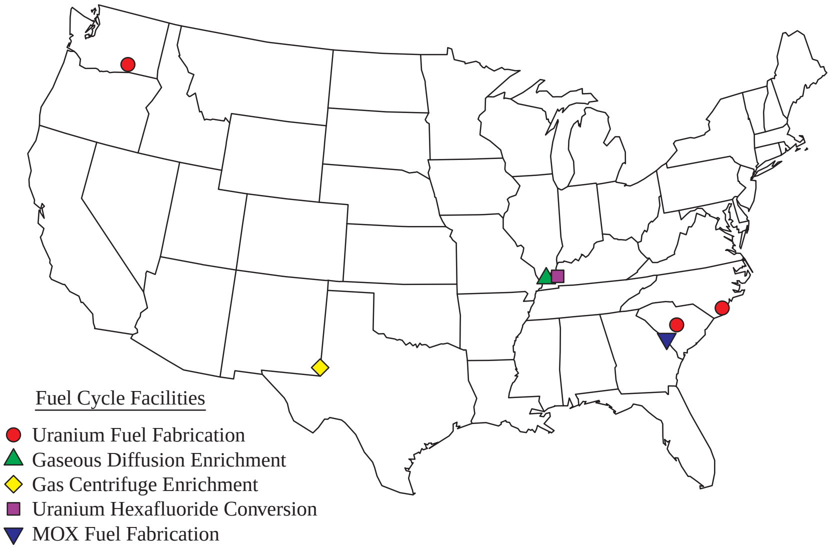
Fuel Cycle Facilities
● Uranium Fuel Fabrication
▲ Gaseous Diffusion Enrichment
◆ Gas Centrifuge Enrichment
■ Uranium Hexafluoride Conversion
▼ MOX Fuel Fabrication

Figure 2.2: U.S. facilities that process nuclear materials at various stages of the nuclear fuel cycle.

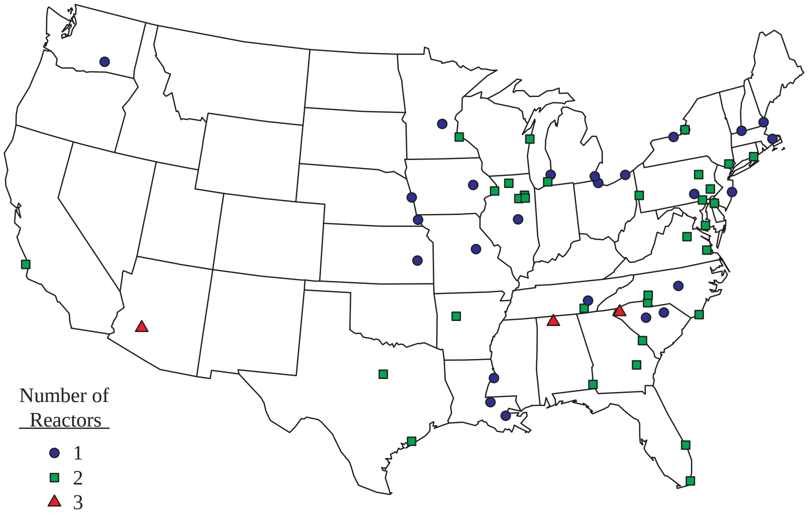

Figure 2.3: Commercial nuclear power reactors operating in the U.S. as of July 2013.

For simplicity, the rest of the thesis focuses on shipments of nuclear material through a truck shipping network. All of our methods apply also to rail networks and combined truck-rail networks, however. No theoretical generality is lost.

CHAPTER 3: DEFINING ADVERSARIAL RISK

This chapter outlines our method for evaluating “adversarial risk.” Adversarial risk measures the potential danger posed by an intelligent adversary that executes a conceivable, worst-case attack on a target of interest.

3.1 A Basic Model of Risk

To build an adversarial model for the transportation of nuclear materials, consider a subset of the overall transportation network: shipping of fresh fuel (by truck) from assembly plants to nuclear reactors. In this *subnetwork*, the material being shipped is reasonably homogeneous as are the transportation containers, which are fresh-fuel casks in this case. Fresh-fuel assemblies may not be the most dangerous material that is shipped within the nuclear fuel cycle, but the fresh-fuel subnetwork is large and diverse, and it is easy to manipulate for purposes of demonstration. The methods also apply to other transportation subnetworks, such as shipping enriched uranium, mixed-oxide (MOX) fuel, and spent fuel.

In an adversarial model, we use “risk” to measure the worst conceivable outcome [6]. A survey of the literature provides two key observations:

Observation 1: Any shipment of nuclear materials could be attacked “successfully,” that is, to yield a direct release of a substantial quantity of nuclear material into the environment [7–9].

Observation 2: Damage (bad publicity, deaths and injuries from chemical and radiation exposure) would be positively correlated with total population in the area in which the material is released [10–12]. It is also clear that cleanup costs would depend strongly on population numbers [13].

Note 1: Lamb and Resnikoff [13] examine a worst-case accident for spent fuel—this worst-case accident is no worse than a worst-case attack—and estimates a cleanup cost in an urban setting at over $13 billion. Fresh fuel would not require such extensive cleanup because of lower levels of radioactivity, but we have not discovered any research that provides cost estimates.

Numerous authors propose the identification of minimum-risk hazardous material (HAZMAT) routes using minimum-cost routing techniques with cost defined as a function of the number of people that might be affected by an accident along a route (e.g., [14–16]). For example, one cost function, applied to the whole route, evaluates *expected consequence*, which is defined as the "population at risk" along the route multiplied by the probability that an accident occurs along that route. Population at risk may be defined as the total population within a certain distance of the route, perhaps inversely weighted by actual distance from the route. ReVelle [16] refers to this general idea as "tons-past-people." Because our focus is a worst-case attack by an intelligent adversary, we use neither probabilities nor total population at risk in creating a "cost function," but rather, use the maximum population that might be affected along a route.

For any point location $\ell \in L$ in the relevant subnetwork s, we apply Observations 1 and 2 to define adversarial risk in an abstract fashion:

$$risk_{s\ell} \approx f_s(pop_\ell), \tag{3.1}$$

where pop_ℓ is the the total population in some to-be-defined region around location ℓ, and where $f_s(\cdot)$ is a monotonically increasing function of population. For an exact measure of risk (e.g., number of deaths, years of cleanup, dollars required for cleanup) the analyst would consult with the references cited above, other existing literature, or develop a problem-specific definition.

Because adversarial risk measures a worst-case outcome, the total risk associated with subnetwork s is simply

$$tot\_risk_s = \max_{\ell \in L} risk_{s\ell} = \max_{\ell \in L} f_s(pop_\ell). \tag{3.2}$$

Thus, in a static situation, for a given subnetwork, we need only focus on the peak population through which shipments move. How that population is measured will depend on the type of material, but the measurement method should be standard for subnetwork s

(through which homogeneous materials are shipped in homogeneous containers).

Note 2: Population is key here because that is what we may have effective control over. For example, by rerouting fuel shipments, the population that might be affected by an attack can change. But then, how can we reduce risk by, say, reducing the quantity of material in a shipment? Without rerouting, population stays the same, the worst-case accident would occur in the same location, and we simply need to apply a different damage function to evaluate risk numerically.

The index of the "worst" subnetwork is simply

$$s_{\max} = \underset{s \in S}{\operatorname{argmax}} \; tot\_risk_s. \tag{3.3}$$

After evaluating risk in a subnetwork, we look for ways to reduce that risk. Risk mitigation for transportation should begin with $s_{\max}$. Suppose that we determine that currently, in the U.S., $s_{\max}$ corresponds to fresh-fuel shipments. We assume that these shipments cannot be made invulnerable to attack, and that reducing their size is impracticable. Splitting single shipments into many smaller shipments would reduce adversarial risk, but might increase accident risk and would require major physical changes in reactors and the refueling process. Consequently, the obvious leverage we have is to reroute shipments through areas with smaller populations. This proposition, which follows from monotonicity of $f_s(\cdot)$, makes solving risk-mitigation problems simple:

Proposition 1: When minimizing adversarial risk within a single subnetwork, maximum population along a link k in that subnetwork may be used as a surrogate for risk on that link.

Let $G = (N,A)$ denote a generic network consisting of nodes N and directed or undirected links A. To illustrate a basic risk-mitigation model, suppose that for subnetwork s, $G_s^h = (N_s, A_s^h)$, $h = 1,\ldots,H$, defines H designs that are under consideration as replacements for the current subnetwork $G_s^0 = (N_s, A_s^0)$. The best design, with respect to adversarial transportation risk, has

$$h_{\min} = \operatorname*{argmin}_{h=1,\ldots,H} \max_{k \in A_s^h} pop_k, \tag{3.4}$$

where pop_k is the maximum population observed along a defined region around link k (for example, a circle centered at a point on the route and encompassing 20 km^2). In the following chapters, this basic concept lets us develop several methods for minimizing adversarial risk by using decoys or changing a network's design.

3.2 Other Models of Adversarial Risk

Other models of risk have been proposed for use in the context of terrorist attacks. We describe two here and point out some of their pitfalls, both in general and in the setting of this thesis.

3.2.1 Probabilistic Risk Analysis

A complex model for evaluating adversarial risk might consider, for instance, the sequence of actions that make up an attack—steal a missile of type A in a foreign country, smuggle a missile of type A into the United States, launch the missile at the target, etc.—each with some probability of success and leading to an overall probability of success. One can also assign probability distributions on the amount of material that would be released for each possible weapon type and the direction and strength of the wind at the time of the attack. Such analysis is classified as *probabilistic risk assessment* (PRA), and PRA has been suggested for "terrorism risk analysis" [17, 18].

The difficulties with such models are well known, for example (a) they place static probability distributions on dynamic human decision making and thereby violate the tenets of game theory, (b) they typically rely on a great deal of "data" derived from subjective estimates from subject matter experts (SMEs), and (c) these data may require enormous effort to obtain and maintain and have uncertain quality [19, 20]. By contrast, our models derive from simple physical models and make minimal assumptions. In our opinion, a complete worst-case analysis should be carried out and be found wanting before attempting to improve that analysis through probabilistic methods.

3.2.2 Attack Difficulty

In a study led by the Sandia National Laboratories, Cipiti *et al.* apply the Risk-Informed Management of Enterprise Security (RIMES) technique to analyze possible attack scenarios on a small modular reactor [21]. This technique seeks to categorize attacks in terms of their difficulty to execute, and then to assess risk by comparing “attack difficulty” with “potential attacker capability.”

Cipiti *et al.* consider 13 dimensions of attack difficulty on a small modular reactor (grouped into two categories: attack preparation and attack execution), and for each of these 13 dimensions they divide difficulty into five levels, with level 1 being the easiest and level 5 the most difficult. For each potential attack, they use the opinions of one or more SMEs to specify the level of difficulty in each of the 13 dimensions. The overall risk then depends on additional SME assessments as to whether any of a set of potential attackers could succeed in overcoming the difficulty level identified in each dimension.

This technique may not require the explicit use of subjective probabilities, and may therefore appear to sidestep some of the criticism of PRA. Nonetheless, it requires at least one SME to assess linearly scaled “difficulty numbers" that (a) are clearly subjective, (b) may be impossible to validate, and that (c) impose a substantial data-collection and data-maintenance burden on the model’s user. By contrast, our models are designed to require little or no subjective input data from SMEs and, although our models can require large amounts of input data (routing and population data), no intrinsic difficulties arise in collecting and maintaining these data.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 4: SUBNETWORKS IN THE DOMESTIC NUCLEAR FUEL CYCLE

This thesis demonstrates adversarial-risk evaluation and adversarial-risk reduction only for the fabricator-to-power-plant subnetwork, or "fresh-fuel subnetwork," within the domestic nuclear fuel cycle. The models apply, however, to any subnetwork that ships a single commodity (e.g., unenriched UF_6). Several "single-commodity subnetworks" can be combined for analysis into a single "multicommodity subnetwork," but this may only make sense if the commodities involved have similar levels of danger associated with them. For example, supposing that unenriched and enriched UF_6 have similar levels of toxicity, then, reducing adversarial risk for the "enriched UF_6 subnetwork" might have little effect if the risk associated with the "unenriched UF_6 subnetwork" were left unchanged. In this case, the two subnetworks should be combined for analysis.

For completeness, we list the single-commodity subnetworks in the U.S. that are relevant now, or may become relevant in the future:

1. **Yellowcake**: This subnetwork includes as its origin nodes various ports of entry and production plants in Wyoming, Nebraska, Utah, Colorado, and Texas. Only Honeywell's Metropolis Works (MTW) facility in Metropolis, Illinois, performs the initial conversion of yellowcake to UF_6, so Metropolis defines the single terminal node in this subnetwork.
2. **Unenriched UF_6**: This simple subnetwork runs from MTW in Metropolis, Illinois, to United States Enrichment Corporation's (USEC) gaseous diffusion plant in Paducah, Kentucky, and URENCO USA's gas centrifuge enrichment plant in Eunice, New Mexico.
3. **Enriched UF_6**: This subnetwork extends from USEC in Paducah, Kentucky, and URENCO in Eunice, New Mexico, to three nuclear fuel fabrication facilities: Areva, Inc., in Richland, Washington (Areva); Global Nuclear Fuels – Americas, LLC, in Wilmington, North Carolina (GNF); and Westinghouse Electric Company, LLC, in

Columbia, South Carolina (Westinghouse).

4. **Fresh fuel**: This subnetwork extends from the three fuel fabricators to the nuclear power plants that burn the fuel, and is described in detail elsewhere in this thesis. Actually, fresh-fuel shipments in the U.S. also include fuel assemblies that are fabricated in the U.S. and shipped to overseas customers [22]. This thesis does not consider such shipments, but a complete adversarial risk analysis for fresh-fuel shipments in the U.S. certainly should.
5. **Spent fuel**: For the most part, spent-fuel shipments in the U.S. domestic fuel cycle have been limited to moving spent fuel for the purpose of consolidating a company's intermediate storage [23]. In the future, any of the following single-commodity subnetworks or combinations thereof could be relevant:
   (a) Dry casks of spent fuel shipped from power plants to intermediate storage.
   (b) Dry casks shipped from power plants and/or intermediate storage to one or more final repositories.
   (c) Dry casks shipped from power plants to one or more reprocessing facilities.
6. **Other materials being reprocessed**: This could include military warheads, domestic or foreign, being processed into fuel (e.g., the "Megatons to Megawatts" program [24]), and spent fuel brought into the United States from foreign countries for reprocessing.
7. **Waste from reprocessing**: If reprocessing becomes relevant, it will generate dry-cask shipments to intermediate storage and/or final repository [25].

The appendix provides more detail on existing subnetworks, but the remainder of the body of the thesis focuses on the fresh-fuel subnetwork.

CHAPTER 5: EVALUATING ADVERSARIAL RISK OR ITS SURROGATE FOR A SUBNETWORK

Because the materials of interest in this thesis are hazardous, these materials typically travel along pre-approved, static routes. It therefore makes sense to evaluate the adversarial risk associated with a static transportation link k of a particular subnetwork s. Following the discussion in the previous chapter, we use this surrogate:

$$d_k = \text{the maximum population that might be affected by an attack on link } k \text{ in subnetwork } s, \quad (5.1)$$

where s is omitted as a subscript because the subnetwork is fixed. This admittedly vague definition will be made more precise, later. To avoid confusion, we call d_k the "damage surrogate" or "damage value."

Note 3: The terms "route" and "link" will be used interchangeably but, strictly speaking, a link between two nodes is the abstraction of the complicated route that moves between two fuel-cycle facilities along roads and past, potentially, many areas of population.

5.1 Damage Values for a "Direct Attack"

Suppose that we determine that a simple, "direct attack" is the key threat: a shipment is attacked with an explosive device of some type, and some of its contents are released into the environment.

The area affected by a direct attack would depend on the material, the amount released, meteorological conditions, etc., but we must focus on a worst case: the discussion and references in Chapter 3 indicate that, in the worst case, most of a shipment's material could be vaporized and released into the environment. Depending on dispersion-plume models (e.g., Harper *et al.* [26], Reshetin [27]), we may assume that material will affect all people within a certain radius of a release site. (A more detailed model might look for the largest population affected if the plume expands centrally, or moves in any particular compass direction.) Then, to compute d_k, we only need to extrapolate census data to points along the corresponding route, and then choose the largest population identified. Using a grid of population cells, our numerical examples use a cruder method to estimate these numbers, but the reader will see that the estimates produced give intuitively sensible results in all tested models.

We begin with a grid of population values divided into latitude-longitude quadrilaterals that are 2.5 arc-minutes on a side [28]. Each quadrilateral (grid cell) has an area of 21.4 km^2 at the equator, which reduces to about 14 km^2 in the southern U.S. and to about 11 km^2 in the northern U.S. This is true since the width of a cell reduces by a factor of $(90-\text{lat})/90$ where "lat" is latitude north in decimal degrees. For simplicity, we assume that an attack would affect the population in a single grid cell of the size seen at the equator. For cells at other latitudes then, we multiply cell population by a correction factor of $90/(90-\text{lat})$ to enable an equal-basis comparison. Finally, to determine the damage value d_k for a given link k , we simply identify the cell with the largest (adjusted) population that intersects the corresponding route. Table 5.1 shows the 10 links with the largest damage values for the hypothetical U.S. fresh-fuel network.

A single grid-square area (11 to 14 km^2) might be too conservative for some nuclear materials. Suppose an appropriate area is roughly nine times the single-cell area. Then, we only need to expand the area of interest to the nine cells that make up the 3×3 block of cells about each relevant point. Table 5.2 shows these values. The top 10 damage values and locations do not change much from Table 5.1, indicating that that the damage surrogate is not particularly sensitive to the data. The biggest difference is that Bronx is now the worst case, corresponding to a shipment that passes through Newark, crosses the George Washington Bridge, and continues into Connecticut, using Interstate Highway 95 (I-95) the whole time. (Of course, we do not know if this route is actually used.) The smaller Newark damage value represents a shipment that crosses the same bridge and then turns north, up I-87, rather than continuing on through the eastern Bronx on I-95.

Table 5.1: The 10 largest damage values and their locations given (a) a direct attack, and (b) the affected population resides in only a single population cell. The related number of affected routes and reactors is also given. For example, nine routes traverse a single location near Chicago, Illinois, where the population data imply a damage value of 261787; those nine routes feed 15 reactors.

Location (nearest city)	**Damage value d_k** (persons)	**Routes** (number)	**Reactors** (number)
Chicago, IL	261787	9	15
Newark, NJ	225895	4	5
Philadelphia, PA	218745	1	1
Washington, DC	184547	4	7
Milwaukee, WI	115225	1	2
Buffalo, NY	103012	1	1
Phoenix, AZ	92792	1	3
Cleveland, OH	78211	1	1
Lincoln, NE	78121	8	15
Chicago, IL (suburbs)	72781	1	2

Table 5.2: The 10 largest damage values for an attack that occurs in a given cell and affects that cell along with the eight adjacent cells. See the caption for Table 5.1 for additional information.

Location (nearest city)	**Damage value d_k** (persons)	**Routes** (number)	**Reactors** (number)
Bronx, NY	2388125	4	5
Chicago, IL	1881620	8	13
Newark, NJ	1219373	1	2
Philadelphia, PA	1172064	1	1
Washington, DC	971233	4	7
Milwaukee, WI	804469	1	2
Phoenix, AZ	666934	1	3
Buffalo, NY	661251	1	1
Cleveland, OH	631157	1	1
Chicago, IL (suburbs)	563459	1	2

5.2 Damage Values for a “Hijacking Attack”

We believe that hijacking a nuclear shipment in the U.S. and moving it any substantial distance would be extremely difficult, given that each shipment is guarded, heavy containers are difficult to move, radio contact or the lack thereof with a hijacked truck should quickly alert authorities of an incident, and that truck or trailer should be easily located and immobilized. Nonetheless, our methods enable consideration of a hijacking scenario.

We assume that it is impossible for a hijacking to go unnoticed, so it is also reasonable to assume that a hijacked truck would be stopped within some short time period, say 30 minutes, after an attack is begun. We assume that a worst-case release of the shipment’s contents would then take place. Thus, to evaluate the damage value for a subnetwork link *k*, we only need to expand the search for a “worst-case population cell” (or “group of cells”) along the route to include the distance that a truck could cover in 30 minutes from any point on link *k*. This could be estimated accurately using road-network and population data, but for demonstration purposes we use a simpler method: assuming again that a release of material would affect only the population in a single cell, we identify the largest population cell within 48.3 km (30 miles) of the route using a straight-line distance calculation. This method yields the damage values displayed in Table 5.3 for the hypothetical fresh-fuel subnetwork described above.

Table 5.3: For a hijacking attack, the 10 largest damage values and their locations. A shipment hijacked on the hypothetical route from Westinghouse to Braidwood is farther than 30 miles from the peak population area of Chicago, Illinois, and a hijacked truck could only reach the suburbs to the south of the Chicago under assumed conditions.

Location	**Damage value d_k**	**Routes**	**Reactors**
(nearest city)	(persons)	(number)	(number)
Bronx, NY	689338	5	7
Chicago, IL	261787	11	19
Philadelphia, PA	218745	4	6
Washington, DC	184547	3	5
Miami, FL	148941	1	2
New Orleans, LA	120858	3	4
Cleveland, OH	112760	1	1
Detroit, MI	111900	1	1
Chicago, IL (suburbs)	110753	1	2
Pittsburgh, PA	109837	2	3

5.3 Reducing Adversarial Risk

The damage-surrogate models above provide objective means of comparing the adversarial risk associated with different routes or scenarios. The next two chapters show how to apply limited resources to reduce risk optimally assuming monotonicity of “true damage” as as function of damage value (as described in Chapter 3). Any of the optimization models could be applied to any subnetwork once an appropriate damage-surrogate is defined. We demonstrate the models on the fresh-fuel subnetwork using the damage surrogate reflected in Table 5.1. An attack at a particular point would affect the population in its respective grid square.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 6: DA1: A GENERAL DEFENDER-ATTACKER MODEL FOR REDUCING ADVERSARIAL RISK IN A TRANSPORTATION SUBNETWORK

This chapter presents a generic mathematical-programming model that uses the damage surrogate to minimize adversarial risk in a transportation subnetwork. The model applies to network design, redesign, modification, and rerouting of certain shipments, all subject to generic resource constraints. We describe the general model in terms of building a subnetwork from scratch, but explain how it applies in the other situations, which are probably more likely to arise in practice (e.g., redesign or simple modifications).

6.1 A General Model: DA1

We assume that a *defender* (fuel-cycle "operators," transporters, regulators, etc.) faces a single adversary or *attacker*, who plans on carrying out a single attack in the transportation system. The defender will build the network, the attacker will observe what has been built and then attack in the most destructive way possible when seen from the viewpoint of the defender. This is a two-stage Stackelberg game, called a "defender-attacker" (DA) model, as described in Brown *et al.* [6]. The worst-case analysis is pessimistic for the defender—will an attacker really be able to carry out a worst-case attack?—but it is prudent. We refer the reader to Brown *et al.* [6], Scaparra and Church [29], Brown *et al.* [30], Alderson *et al.* [31], and the references therein for other applications of DA models or the related defender-attacker-defender (DAD) models to problems of infrastructure design and/or defense.

A solution to the following model will identify a minimum-risk subnetwork in which each origin node is connected uniquely to a source and subject to capacity constraints at each origin node and each destination node. Consequently, the subnetwork is bipartite. Such a model could be used, for example, to design a fabricator-to-power-plant subnetwork from scratch. But, it could also be used to make a limited number of changes to an existing subnetwork to reduce risk, or to guide rerouting decisions. Note that the capacity constraints may simplify greatly in most applications. For instance, in the fresh-fuel subnetwork, the capacity constraints at a destination node (i.e., at a power plant) may simplify to “Attach exactly one source (i.e., fuel fabricator) to this power plant.”

The network models here differ from those described in traditional capacitated network design; for example, see Magnanti and Wong [32] and the references therein. Such designs typically use binary variables to represent construction of a network and continuous variables to represent activities that may use the constructed network’s capacity. For example,

$$\sum_h r_{hk} y_{hk} \quad \leq \quad \bar{r}_k x_k;\ x_k \in \{0,1\};\ y_{hk} \geq 0 \ \forall\ h \text{ where } r_{hk} > 0 \ \forall\ h$$

might imply that if link k is constructed ($x_k = 1$), then the sum of all activities h, converted to a common unit of measurement ($\sum_h r_{hk} y_{hk}$) must not exceed the constructed capacity of the link which is $\bar{r}_k$. But if the link is not constructed ($x_k = 0$), then no activities may take place on that link at all because $\sum_h r_{hk} y_{hk} \leq 0$. By contrast, one of our model’s “constructed links” k is not a physical link, but essentially a contract for a fixed level of activity, for example, the shipping of u fuel assemblies each year between a fabricator and a nuclear power plant. The creation of this link tells us exactly the amount of resource that will be consumed at the fabricator for instance (i.e., u). Thus, the model presented below incorporates binary “link-construction variables” x_k without any continuous “link activity variables.”

Indices and Index Sets

$i \in N^S$	origin nodes in a bipartite subnetwork
$j \in N^T$	destination nodes in a bipartite subnetwork; $N^S \cap N^T = \emptyset$
$i, j \in N$	all nodes in a bipartite subnetwork; $N = N^S \cup N^T$
$k \in A$	links a subnetwork; $k = (i, j)$ where $i \in N^S$, $j \in N^T$
$i(k),\ j(k)$	respectively, the origin and destination nodes for link $k \in A$
$G = (N, A)$	the bipartite subnetwork, also written as $G = (N^S, N^T, A)$
$k \in A^S(i)$	links directed out of node $i \in N^S$
$k \in A^T(j)$	links directed into node $j \in N^T$

$r \in R$ resource types

Data

d_k damage surrogate for link $k \in A$

$\underline{u}_{ir}^{S}$, $\bar{u}_{ir}^{S}$ respectively, the minimum and maximum allowable capacity utilization for resource r at $i \in N^S$

$\underline{u}_{jr}^{T}$, $\bar{u}_{jr}^{T}$ respectively, the minimum and maximum allowable capacity utilization for resource r at $j \in N^T$

u_{kr}^{S} capacity utilization of resource r at i given that $k \in A^S(i)$ is selected

u_{kr}^{T} capacity utilization of resource r at j given that $k \in A^T(j)$ is selected

Variables

x_k 1 if the new network design includes link k, and 0 otherwise

z maximum of damage surrogates across all links

Formulation

$$\begin{aligned}
\textbf{DA1}: \ \min z & & \qquad (6.1)\\
\text{s.t. } z - d_k x_k &\geq 0 \ \forall\, k \in \ A & \qquad (6.2)\\
\underline{u}_{ir}^{S} \leq \sum_{k \in A^S(i)} u_{kr}^{S} x_k &\leq \bar{u}_{ir}^{S} \ \forall\, i \in N^S,\ r \in R & \qquad (6.3)\\
\underline{u}_{jr}^{T} \leq \sum_{k \in A^T(j)} u_{kr}^{T} x_k &\leq \bar{u}_{jr}^{T} \ \forall\, j \in N^T,\ r \in R & \qquad (6.4)\\
x_k &\in \{0,1\} \ \forall\, k \in A & \qquad (6.5)
\end{aligned}$$

The objective function (6.1), in conjunction with constraints (6.2), minimizes the maximum surrogate damage across all links in the selected subnetwork design. Constraints (6.3) place lower and upper limits on the capacity utilization that the network design places on origin nodes; constraints (6.4) are analogous for destination nodes. The user is free to add constraints to represent more complicated logical relations among the links, but the application to fresh-fuel shipments in the following section actually simplifies the model.

6.2 An Application of DA1: Recontracting

This section describes applications of **DA1** to reduce adversarial risk, using the fresh-fuel subnetwork as an example. The network is modified by changing fabricator-to-power-plant assignments (fuel-supply contracts). The construction of the realistic routes used for testing here has already been described in Section 5.1. The appendix describes the collection and construction of other data needed in these models.

Adversarial risk in a subnetwork can be reduced by restructuring a network so that maximum population across all routes is reduced. For illustrative purposes, we imagine here that a central authority arranges all fuel-supply contracts, and any or all contracts could be renegotiated so that, in effect, certain high-risk routes are replaced by lower-risk ones. We require only that the total capacity utilization of a fabricator stay within ±10% of its current capacity as estimated in the appendix, and that each power plant be assigned to one fabricator. **DA1** simplifies then as follows.

Modified data

$\bar{A}$ links $k \in A$ that correspond to new contracts

$\bar{n}$ maximum number of new contracts

$\underline{n}_i$, $\bar{n}_i$ respectively, the minimum and maximum number of fuel assemblies that fabrication facility at $i \in N^S$ may produce in a year

$n_{j(k)}$ number of reactors at power facility located at $j(k) \in N^T$

Formulation

$$
\begin{array}{rrcll}
\mathbf{DA1-Fuel}: & \min\limits_{\mathbf{x},z} z & & & (6.6) \\
& \text{s.t. } z - d_k x_k & \geq & 0 \ \forall\, k \in \ A & (6.7) \\
\underline{n}^S_{ir} \ \leq & \sum\limits_{k \in A^S(i)} n_{j(k)} x_k & \leq & \bar{n}^S_{ir} \ \forall\, i \in N^S & (6.8) \\
& \sum\limits_{k \in A^T(j)} x_k & = & 1 \ \forall\, j \in N^T & (6.9) \\
& \sum\limits_{k \in \bar{A}} x_k & \leq & \bar{n} & (6.10) \\
& x_k & \in & \{0,1\} \ \forall\, k \in A & (6.11)
\end{array}
$$

Using the existing contract structure defined in Table A.1, and using the single-cell "direct attack" as defined in Section 5.1, Table 6.1 displays the maximum "affected populations" observed along current shipping routes or "links."

Table 6.1: Routes with the largest damage values. For example, nine routes traverse the same road segment near Chicago, Illinois, which imposes the largest damage value of any location on any route.

Location	Chicago, IL	Newark, NJ	Phil., PA	Wash., DC
Damage	261787	225895	218745	184547
Number of routes	9	4	1	4
Number of reactors	15	5	1	7

Using **DA1-Fuel** and allowing any and all business contracts to be renegotiated to minimize adversarial risk produces the damage-surrogate results shown in Table 6.2.

Table 6.2: Largest damage values after recontracting.

Location	Newark, NJ	Phil., PA	Wash., DC	San Jose, CA
Damage	225895	218745	184547	142297
Number of routes	5	1	4	1
Number of reactors	7	1	7	2

The solution displayed in in Table 6.2 actually involves recontracting a majority of the contracts, yet the overall risk for the new network only drops from 261787 to 225895. The difficulty is this: although allowing changes in any supplier contract substantially reduces the threat to Chicago, a large reduction is risk is impossible because of the need to transport fuel up the east coast, through New Jersey. We add the requirement that, in order to change a business contract, there must be a decrease in the overall risk to the for the new network. Thus, what may be viewed as the best solution here (see details in Table 6.3) only changes 13 routes. Specifically, it eliminates the nine shipments passing through Chicago and modifies four others to reduce the maximum damage value from 261787 to 225895, the same as the more resource-intensive solution reflected in Table 6.2. The results here show that **DA1-Fuel** will allocate resources to lower damage values for the second-worst route, the third-worst route, etc., but this extra resource does not reduce overall risk for this scenario because the maximum damage value cannot drop below 225895.

Table 6.3: Recontracting. Thirteen nuclear fuel supply contracts change. Additional changes to business contracts do not lower the overall risk for the network. While avoiding Chicago, the worst-case damage of 225895 occurs for shipments traveling on I-95 past Newark, New Jersey.

	Existing		Optimal	
Reactor site	**Fabricator**	**Damage value**	**Fabricator**	**Damage value**
Byron	Westinghouse	72781	Areva	57167
Calvert Cliffs	Areva	261787	Westinghouse	52819
Comanche Peak	Westinghouse	70099	Areva	70297
Davis-Besse	Areva	261787	Westinghouse	49714
Millstone	Areva	261787	Westinghouse	225895
North Anna	Areva	261787	Westinghouse	52819
Palisades	Areva	261787	GNF	65499
Palo Verde	Westinghouse	92792	Areva	87050
Prairie Island	Westinghouse	261787	Areva	83228
Sequoyah	Westinghouse	70099	Areva	78121
Surry	Areva	261787	Westinghouse	41611
Susquehanna	Areva	261787	Westinghouse	41611
Three Mile Island	Areva	261787	Westinghouse	64584

6.3 Simple Rerouting: A Greedy Approach

While mathematical programming can be used to address adversarial-risk reduction on a large scale, simply rerouting the fuel shipments around the points with the largest damage values can reduce the overall risk. A systematic "greedy algorithm" applies here, one that is clearly optimal under certain conditions:

Step 1: Find the route with largest damage value.

Step 2: Since that implies the adversarial risk for the whole subnetwork, the damage value for this route must be reduced to reduce overall risk.

Step 3: Assuming you have additional "rerouting resource," reroute the link with the largest damage value, and return to Step 1.

For the initial matrix of fuel-fabricator-to-power-plant routes, Chicago, Illinois, defines overall risk through nine routes serving 15 reactors that traverse Interstate Highway I-94.

With the intent to eliminate the Chicago's damage value of 261787, we create nine alternate routes that instead use I-74 through Champaign, Illinois. As shown in Table 6.4, worst-case damage is reduced significantly without adding much travel distance.

Table 6.4: These routes all define the maximum damage value of 261787 in the baseline ("initial") system. To reduce overall risk by rerouting, all nine routes through Chicago must be modified in some way. We restrict rerouting decisions to use I-74 through Champaign, Illinois. The Millstone-Areva route now defines risk for this subnetwork because its damage value of 220173 is greatest.

Reactor site	**Fabricator**	**City**	**Damage value**	**Extra miles**
Calvert Cliffs	Areva	Washington, DC	90983	75
Davis-Besse	Areva	Toledo, OH	59027	170
Millstone	Areva	Bronx, NY	220173	127
North Anna	Areva	Indianapolis, IN	48920	44
Palisades	Areva	Peoria, IL	47218	384
Prairie Island	Westinghouse	Rockford, IL	57167	42
Surry	Areva	Richmond, VA	52819	28
Susquehanna	Areva	Indianapolis, IN	48920	151
Three Mile Island	Areva	Columbus, OH	72548	88

The same process repeats to eliminate the next worst-case point of attack, which are routes that transit north on I-95 between Newark, New Jersey, and New York City. The procedure could continue repeating for other cities until, say, a predetermined acceptable damage level for the subnetwork is reached.

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 7: DA2: REDUCING EXPECTED RISK WITH DECOY SHIPMENTS

A solution to **DA1** structures or restructures a subnetwork to minimize adversarial risk, with risk viewed as a deterministic function. If we allow probability to come into play, decoy shipments can be used to reduce *expected risk*. We are loathe to allow subjective, uncontrollable probabilities into a model, but here the probabilities are straightforward to compute and are under our control.

7.1 Allocating Decoys Optimally: DA2

This section uses this additional or modified notation.

x_k the number of decoys assigned to each shipment on link k, 0 otherwise

$\bar{x}_k$ a maximum value for x_k (set by planners)

m_k (length of link k in miles) × (number of shipments made per year on link k) [miles/year]

$\bar{m}$ total budget for decoys [miles/year]

n_x maximum total number of decoys

Assumption 1: Damage on each link $k \in A$ is computed as $d_k = f(pop_k) = c \cdot pop_k$. That is, damage is a linear function of population.

Focusing on a single link k, damage is computed through a function $d_k = f(pop_k)$. Expected damage equals damage. Suppose that for every shipment along k, we send x_k decoy shipments. The attacker has one chance to strike on this link, so assuming that a decoy shipment is indistinguishable from a real one, the probability of a successful attack is $1/(1+x_k)$. (Note that x_k is being used for a different purpose here than in previous sections.) For simplicity, we assume that a single truck carries each shipment and that any decoy trucks follow the same route as a real shipment. The following model results.

$$\textbf{DA2}-\textbf{Decoy0} \quad z^* = \min_{\mathbf{x}\in X_{\text{Decoy}}} \max_{k\in A} d_k/(1+x_k), \tag{7.1}$$

where

$$X_{\text{Decoy}} \equiv \left\{x_k \in \{0,\ldots,\bar{x}_k\} \forall k \in A \mid \textstyle\sum_{k\in A} m_k x_k \le \bar{m}\right\}. \tag{7.2}$$

Making the reasonable assumption that $d_k > 0$ for all $k \in A$, the nonlinear model **DA2-Decoy0** has the same solution as this integer linear program:

$$\begin{aligned}
\textbf{DA2}-\textbf{Decoy1} \quad (z^*)^{-1} \;=\; v^* \;=\; \min_{\mathbf{x},v}\; & v & & & (7.3)\\
\text{s.t. } v \;&\ge\; d_k^{-1}\cdot(1+x_k)\;\forall k\in A & & & (7.4)\\
\sum_{k\in A} m_k x_k \;&\le\; \bar{m} & & & (7.5)\\
\sum_{k\in A} x_k \;&\le\; n_x & & & (7.6)\\
0 \;\le x_k \;&\le\; \bar{x}_k,\text{ integer } \forall k\in A & & & (7.7)
\end{aligned}$$

If the decoys are controlled or owned by the originating nodes $i \in N^S$ (suppliers), then constraint (7.5) would simply be replaced with these constraints:

$$\sum_{k\in A^S(i)} m_k x_k \;\le\; \bar{m}_i \;\forall\; i \in N^S, \tag{7.8}$$

where $\bar{m}_i$ denotes the number of decoy miles available at node i.

7.2 A Sample Application of Decoys

In this section, we apply **DA2** to the same fuel-fabricator-to-power-plant matrix used in previous chapters. Imagine an idealized situation in which (a) a central authority funds decoy shipments of fresh fuel across all fabricators, (b) refueling periods are the same for every reactor, (c) every power-generating stations that operate multiple reactors receive a shipment for each reactor, and (d) one mile of a decoy shipment on any route costs the same. Because of the common refueling period and single cost, we can discuss the allocation of "decoy miles" rather than "decoy miles per year" or "decoy dollars per year."

The no-decoy case produces the expected damage value of 261787, which occurs for any of the 15 shipments that pass through Chicago, Illinois, on I-94. ("Expected damage value" is equivalent to "damage value" with no decoys.) To achieve any reduction in expected damage, decoy-miles must be assigned to cover each of those 15 shipments. By allocating 36489 decoy miles then, the expected damage associated with an attack in Chicago drops to $261787/2 = 130893.5$, and thus expected damage is defined by the remaining maximum damage value, which is 225895 at Newark, New Jersey. We could then determine the total decoy miles required to cover the five shipments that pass through Newark, and further reduce the damage value to 218745, which is the value imposed by the shipment moving near Philadelphia, Pennsylvania.

This seemingly manual process of optimization can be automated by running the model **DA2** for increasing values of the resource, total decoy-miles. Table 7.1 shows how optimally allocated, increasing levels of decoy-miles reduce expected damage. Note how Chicago again becomes "the long pole in the tent" once sufficient decoy miles are allocated to routes passing through or near Washington, D.C. The "Chicago routes" must then receive a second allocation of decoys to reduce expected damage further.

Table 7.1: Optimal reductions in expected damage as total decoy-miles increase.

Location	**Expected**	**Decoy**	**Max decoys**	**Decoy miles**	
	damage	**shipments**	**per route**	**min**	**max**
Chicago, IL	261787	0	0	0	36488
Newark, NJ	225895	15	1	36489	40567
Philadelphia, PA	218745	20	1	40568	41116
Washington, DC	184547	21	1	41117	44907
Chicago, IL	130894	28	1	44908	81396
Milwaukee, WI	115225	43	2	81397	84648

THIS PAGE INTENTIONALLY LEFT BLANK

CHAPTER 8: CONCLUSIONS

Different authorities will have different measures of "damage" that an adversary might cause by attacking a shipment of nuclear material within a U.S. nuclear fuel cycle. Theft seems extremely unlikely given the great bulk of the containers used for shipping most nuclear materials, so this thesis has focused on a "direct attack" that that causes a release of vaporized material into the atmosphere, probably through the use of some explosive device applied right on the shipping route. We argue that "population affected" by an attack is a good surrogate for damage because (a) most any standard damage measure, say "economic losses," is likely to be monotonically increasing in population affected and (b) allocating resources to minimize the damage surrogate will also minimize the "real" measure of worst-case damage.

"Population affected" will certainly depend on the details of an attack, the amount of material released, weather conditions, etc. But, we propose and justify a worst-case view of an attack that makes calculations possible: any shipment can be successfully attacked and the bulk of its cargo released into the environment. Although difficult to obtain, it is well within the realm of possibility that a terrorist organization could obtain an explosive weapon that would cause the catastrophic release of the shipment's contents into the atmosphere.

Computing population affected involves applying standard plume models for movement of material through the air and some model of toxicity. We do not use any actual plume model, but demonstrate computational techniques by identifying the largest population within a region of pre-specified size anywhere along a shipment route. We also demonstrate how the model modifies to handle a hijacking attack in which a cargo is hijacked, moved to a new location, and then detonated.

Given a surrogate measure of damage (i.e., an adversarial-risk-assessment method), we then develop models to minimize worst-case damage or expected worst-case damage using limited resources. In effect, this is optimized, adversarial-risk reduction; we optimize using sequential-game models, called "defender-attacker models." For example, we can minimize the worst-case damage subject to the rerouting of a given number of shipments, or we can minimize expected worst-case damage by applying limited decoy shipments. Such a model could also be used to show how, for instance, increasing the number of suppliers for a material could reduce risk, by replacing “dangerous routes” with less-dangerous ones. We demonstrate these methods on a realistic model of the subnetwork that transports fresh-fuel assemblies throughout the U.S. Fresh-fuel assemblies are not the most dangerous material that are shipped in a nuclear fuel cycle, but the subnetwork is large and it yields interesting case studies.

We have provided a framework for evaluating any part (subnetwork) of the transportation network that ships nuclear materials for a U.S. nuclear fuel cycle. We have demonstrated intuitively appealing results on realistic but largely artificial route data and simplified models of the population that would be affected by the release of material. We hope that regulators, physicists, geographers, and others who have access to actual data and expertise in the key physical models will be able to obtain new insights into adversarial risk, and be able to help reduce it by applying our methods.

Appendix: Realistic Test Data

This appendix describes how the data used in this thesis were gathered and/or generated. We describe the collected and generated data based on our level of certainty in its accuracy, from “known” to “unknown,” with varying degrees of uncertainty in between. The “knowns” are easily obtainable from a simple search on the internet, such as facility names and their geographical coordinates. “Unknowns” are unavailable to the general public due to their sensitive nature, such as the specific highway routes that a nuclear fuel convoy takes between a fuel fabricator and a nuclear power station.

The data we gather and create describe the fresh-fuel shipping network.

Known: Facility locations

The facility types relevant to the fresh-fuel network are nuclear reactor fuel fabricators and nuclear power plants. The latitude and longitude for each location are used for determining transportation routes.

Nuclear reactor fuel fabricators

Nuclear reactor fuel is fabricated at three sites: Areva Inc., in Richland, Washington; Global Nuclear Fuel – Americas, LLC, a joint operation of General Electric Energy, Toshiba, and Hitachi, in Wilmington, North Carolina; and Westinghouse Electric Company, LLC, in Columbia, South Carolina.

Nuclear power plants

At the start of 2013, there were 104 nuclear reactors licensed for power generation, operating on 65 different sites. In the first half of the year, four reactors at three different sites were retired: Duke Energy’s Crystal River Nuclear Plant, shut down since September 26, 2009, announced closure on February 5, 2013; Dominion Resources’ Kewaunee Power Station, announced closure on October 22, 2012, and shut down on May 7, 2013; and Southern California Edison’s San Onofre Nuclear Generating Station (two reactors), shut down since January 31, 2012, announced closure on June 7, 2013. Constellation/Exelon’s Nine Mile Point Nuclear Station (two reactors) and Entergy’s James A. FitzPatrick Nuclear Power Plant share the same site in Scriba, New York. PSEG Nuclear’s Hope Creek

Nuclear Generating Station (two reactors) and Salem Nuclear Generating Station share the same site in Hancock's Bridge, New Jersey.

We use the latitude and longitude coordinates for each power plant location, as well as the number of reactors at each station. A total of 100 nuclear reactors are operating at 62 independently licensed sites.

Partly known: Fabricator capacities

According to the World Nuclear Association, the production capacities of light water reactor (LWR) fuel, in metric tons per year, are: Areva's Richland facility, 1200; Global Nuclear Fuel's Wilmington facility, 750; and Westinghouse's Columbia facility, 1500 [33]. Assuming no import or export of nuclear fuel rods or assemblies, we convert these capacities to a percentage of total fabrication capacity: Areva, 35%; GNF, 22%; and Westinghouse, 43%. The number of reactors supplied by a fuel fabricator is divided by the total number of reactors in operation to determine the fuel fabricator's capacity percentage. These percentages are used as "goals" when considering how many reactors each fabricator can supply. Differences in rated reactor thermal output (in MWt) or actual refueling mass (in kg) are not considered when assigning a shipment demand to a fuel fabricator.

Partly known: Fuel fabricator to power-plant assignments

News releases on the awarding of fuel-supply contracts establish some actual fabricator-to-power-plant assignments. For facilities for which we could not find contracting announcements, we make assumptions based on the type of reactor and the owner/operator corporation, ensuring the total assignments to each fabricator are close to that fabricator's percent capacity. It is important to note that, while the corporations involved in the nuclear fuel supply chain may choose to provide news releases pertaining to their business endeavors, we find relatively few actual notices of fabricator/power-plant contracts, so the assignments we use are substantially notional.

Table A.1 shows the notional business contract structure used in computational tests.

Table A.1: Partly hypothetical fuel-fabricator-to-power-plant assignments, with number of reactors at each power plant. These assignments define the baseline fresh-fuel subnetwork in computational tests.

Fabricator	Nuclear station	Reactors	Fabricator	Nuclear station	Reactors
Areva	Arkansas Nuc. One	2	GNF	Oyster Creek	1
Areva	Browns Ferry	3	GNF	Peach Bottom	2
Areva	Brunswick	2	GNF	Perry	1
Areva	Calvert Cliffs	2	GNF	Pilgrim	1
Areva	Catawba	2	GNF	River Bend	1
Areva	Davis-Besse	1	GNF	Vermont Yankee	1
Areva	Dresden	2	Westinghouse	Beaver Valley	2
Areva	Fort Calhoun	1	Westinghouse	Braidwood	2
Areva	McGuire	2	Westinghouse	Byron	2
Areva	Millstone	2	Westinghouse	Callaway	1
Areva	Monticello	1	Westinghouse	Comanche Peak	2
Areva	North Anna	2	Westinghouse	D.C. Cook	2
Areva	Oconee	3	Westinghouse	Diablo Canyon	2
Areva	Palisades	1	Westinghouse	Farley	2
Areva	Quad Cities	2	Westinghouse	Ginna	1
Areva	Robinson	1	Westinghouse	Hope Creek	1
Areva	Shearon Harris	1	Westinghouse	Indian Point	2
Areva	Surry	2	Westinghouse	Palo Verde	3
Areva	Susquehanna	2	Westinghouse	Point Beach	2
Areva	Three Mile Island	1	Westinghouse	Prairie Island	2
GNF	Clinton	1	Westinghouse	Salem	2
GNF	Columbia	1	Westinghouse	Seabrook	1
GNF	Cooper	1	Westinghouse	Sequoyah	2
GNF	Duane Arnold	1	Westinghouse	South Texas	2
GNF	Fermi	1	Westinghouse	St. Lucie	2
GNF	FitzPatrick	1	Westinghouse	Summer	1
GNF	Grand Gulf	1	Westinghouse	Turkey Point	2
GNF	Hatch	2	Westinghouse	Vogtle	2
GNF	LaSalle	2	Westinghouse	Waterford	1
GNF	Limerick	2	Westinghouse	Watts Bar	1
GNF	Nine Mile Point	2	Westinghouse	Wolf Creek	1

Largely unknown: Routing of fuel shipments

We cannot identify appropriate, approved HAZMAT routes that are used for a shipping nuclear fuel, except in a few states that publish detailed information. Therefore, for simplicity and consistency, we use the "Get Directions" feature in Google Earth to produce a transportation route from each fuel fabricator to each of its assigned "customers." Each route is based on fastest travel time, so this places shipments mostly on high-capacity highways and interstate freeways, which seems to be realistic.

To demonstrate "realistic," consider the Google Earth route from from Areva to Arkansas Nuclear One as it passes through the state of Colorado, shown by a heavy dark line in Figure A.1. The Colorado Department of Public Safety publishes a map of roads approved for shipping hazardous materials, and the roads colored green in Figure A.2 are those approved for nuclear materials [34]. Note that the Google Earth route follows the Colorado-approved roads fairly closely, with the only difference being that the Google Earth route avoids Denver's city center.

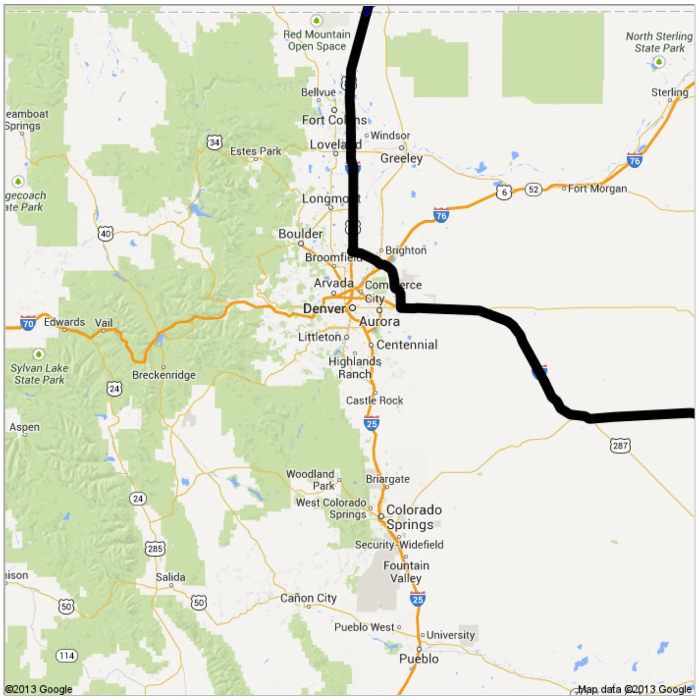

Figure A.1: Google Earth routing from Areva to Arkansas Nuclear One as it transits Colorado, shown as a heavy black line.

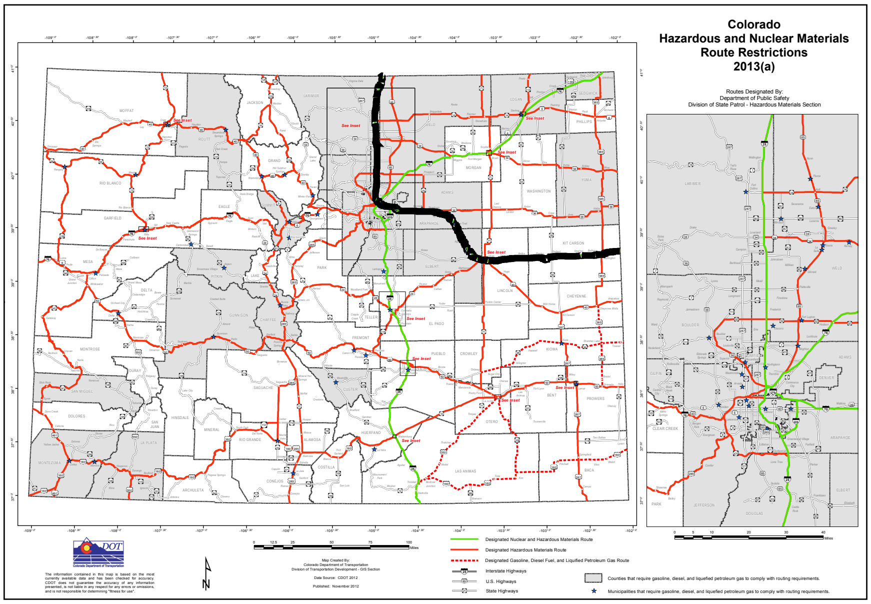
Colorado
Hazardous and Nuclear Materials
Route Restrictions
2013(a)
Routes Designated By:
Department of Public Safety
Division of State Patrol - Hazardous Materials Section
See Inset
Designated Nuclear and Hazardous Materials Route
Designated Hazardous Materials Route
Designated Gasoline, Diesel Fuel, and Liquified Petroleum Gas Route
Interstate Highways
U.S. Highways
State Highways
Counties that require gasoline, diesel, and liquefied petroleum gas to comply with routing requirements.
Municipalities that require gasoline, diesel, and liquefied petroleum gas to comply with routing requirements.
Miles

Figure A.2: Colorado hazardous and nuclear materials route restrictions. Approved nuclear materials routes are shown in green. A shipment from Areva to Arkansas Nuclear One might take the route that is highlighted in black over the approved nuclear materials routes on I-25 and I-70. Along with Figure A.1, this demonstrates that the "fastest-path" routing from Google gives a partial route that is plausible given HAZMAT road restrictions. After [34].

Unknown: Total population affected by a worst-case attack

As a surrogate for worst-case damage that could be incurred along a link in a subnetwork, we have proposed "the population affected." Of course, exact calculations of this will depend on the subnetwork, the material being shipped, and other factors. A reasonable approximation of population affected at a point location would be the population in a circular region of given area centered about that point. Erkut and Verter [14] discuss a "danger circle" as a simplification of a PRA approach to transportation of HAZMAT. To avoid complicated geographical calculations, we assume that

1. A grid is laid across the region of interest, with each (roughly) square region corresponding to a quadrilateral formed by the cell's latitude and longitude, and
2. Only the population of a grid square would be affected by an attack in that square.

Thus, d_k for link k may be computed by identifying all squares that intersect the corresponding route and recording the maximum population among those.

To demonstrate, we use the populations from the database called “Gridded Population of the World, Version 3 (GPWv3): Population Count Grid” [28]. This database provides populations from the 2000 U.S. Census, adjusted to match U.N. totals. The grid resolution is 2.5 arc-minutes per square or “cell.” The population is corrected as a function of area affected, as described in Section 5.1.

Route coordinates are computed as described above so that route-block intersections are straightforward to establish. The length of each route, used elsewhere, is computed during this process, also. For the hypothetical fresh-fuel subnetwork, Table 5.1 displays the ten routes with highest potential damage. Chapter 5 also describes how this model modifies to handle worst-case attacks that would release material over a larger area than a single cell and how it extends to hijacking attacks.

Data for other subnetworks

We include a discussion of other data that might be used for evaluating adversarial risks in subnetworks we do not consider.

Uranium Enrichment

Domestic enrichment of uranium occurs at two sites: United States Enrichment Corporation’s gaseous diffusion plant, in Paducah, Kentucky, and URENCO USA’s gas centrifuge enrichment plant in Eunice, New Mexico. Enriched uranium hexafluoride is shipped to each of the three fuel fabrication sites. An application of the recontracting model of Section 6.2, while initially seeming overly simplistic given only two supply nodes, could be more significant if additional uranium enrichment sites are built, or if one considers the ports of entry of imported enriched uranium. Simple rerouting using the “greedy algorithm,” as shown in Section 6.3, could easily be applied to this small subnetwork. The decoy model of Chapter 7 could be employed here, if a correction factor were applied to the damage surrogate that accounts for the change in anticipated severity of an attack on a uranium hexafluoride shipping cask when compared to an attack on a fresh fuel assembly cask. An application of the recontracting model would require building additional uranium enrichment sites or considering the ports of entry of imported enriched uranium.

Mixed Oxide Fuel

A MOX fuel production facility is under construction at DoE's Savannah River Site, in Aiken, South Carolina. The Tennessee Valley Authority (TVA) has expressed interest in using MOX fuel. TVA operates the Browns Ferry Nuclear Power Plant (three reactors), near Athens, Alabama; Sequoyah Nuclear Generating Station (two reactors), near Soddy-Daisy, Tennessee; and Watts Bar Nuclear Generating Station, near Spring City, Tennessee. Unless domestic production of MOX fuel increases to multiple sites, the recontracting model will not apply. Similar to the uranium-enrichment case, simple rerouting could be employed, as well as the decoy model, provided a correction factor is applied to the damage function.

Spent Fuel to Repository

No repository exists in the U.S., but the issues surrounding such shipments have been well studied during the failed attempt to create a repository at Yucca Mountain, Nevada; for example, see Riddle *et al.* [35]. Standard rail shipments of heavy casks would probably apply here making analysis fairly easy.

THIS PAGE INTENTIONALLY LEFT BLANK

References

[1] National Research Council, *Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex*. Washington, DC: The National Academies Press, 2011.

[2] S. Weinberger, “Laser plant offers cheap way to make nuclear fuel,” *Nature*, vol. 487, no. 7405, pp. 16–17, 2012.

[3] J. Paisner, “Atomic vapor laser isotope separation,” *Applied Physics B*, vol. 46, no. 3, pp. 253–260, 1988.

[4] A. Worrall, “Utilization of used nuclear fuel in a potential future US fuel cycle scenario,” in *WM2013 Conference Proceedings*, Phoenix, AZ, Feb. 24–28, 2013. [Online]. Available: http://info.ornl.gov/sites/publications/files/Pub40177.pdf

[5] J. Schecker, “Yucca Mountain: The million-year promise,” *1663 Los Alamos Science and Technology Magazine*, pp. 14–19, Dec. 2008.

[6] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, “Defending critical infrastructure,” *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.

[7] J. Magill, D. Hamilton, K. Lützenkirchen, M. Tufan, G. Tamborini, W. Wagner, V. Berthou, and A. Von Zweidorf, “Consequences of a radiological dispersal event with nuclear and radioactive sources,” *Science and Global Security*, vol. 15, no. 2, pp. 107–132, 2007.

[8] R. Halstead, “Radiation exposures from spent nuclear fuel and high-level nuclear waste transportation to a geologic repository or interim storage facility in Nevada,” State of Nevada Nuclear Waste Project Office, Carson City, NV, Tech. Rep., Apr. 1997. [Online]. Available: http://www.state.nv.us/nucwaste/trans/radexp.htm

[9] A. Mannan, “Preventing nuclear terrorism in Pakistan: Sabotage of a spent fuel cask or a commercial irradiation source in transport,” The Henry L. Stimson Center, Washington, DC, Tech. Rep., Apr. 2007. [Online]. Available: http://www.stimson.org/images/uploads/research-pdfs/VFMannan.pdf

[10] G. Sandquist, V. Rogers, A. Sutherland, and G. Merrel, “Exposures and health effects from spent nuclear fuel transportation,” Rogers and Associates Engineering Corporation, Salt Lake City, UT, Tech. Rep., Nov. 1985, RAE-8339/12-1.

[11] V. Kumar, R. Goel, R. Chawla, M. Silambarasan, and R. Sharma, "Chemical, biological, radiological, and nuclear decontamination: Recent trends and future perspective," *Journal of Pharmacy And Bioallied Sciences*, vol. 2, no. 3, p. 220, 2010.

[12] B. Biwer, F. Monette, L. Nieves, and N. Ranek, "Transportation impact assessment for shipment of uranium hexafluoride (UF_6) cylinders from the East Tennessee Technology Park to the Portsmouth and Paducah gaseous diffusion plants," Argonne National Laboratory, Argonne, IL, Tech. Rep., Oct. 2001, ANL/EAD/TM-112.

[13] M. Lamb and M. Resnikoff, "Radiological consequences of severe rail accidents involving spent nuclear fuel shipments to Yucca Mountain: Hypothetical Baltimore rail tunnel fire involving SNF," Radioactive Waste Management Associates, New York, NY, Tech. Rep., Sep. 2001. [Online]. Available: http://www.state.nv.us/nucwaste/news2001/nn11459.pdf

[14] E. Erkut and V. Verter, "Modeling of transport risk for hazardous materials," *Operations Research*, vol. 46, no. 5, pp. 625–642, Sep./Oct. 1998.

[15] E. Erkut and A. Ingolfsson, "Catastrophe avoidance models for hazardous materials route planning," *Transportation Science*, vol. 34, no. 2, pp. 165–179, May 2000.

[16] C. ReVelle, J. Cohon, and D. Shobrys, "Simultaneous siting and routing in the disposal of hazardous wastes," *Transportation Science*, vol. 25, no. 2, pp. 138–145, May 1991.

[17] H. Rosoff and D. Von Winterfeldt, "A risk and economic analysis of dirty bomb attacks on the ports of los angeles and long beach," *Risk Analysis*, vol. 27, no. 3, pp. 533–546, 2007.

[18] B. Ezell, S. Bennett, D. Von Winterfeldt, J. Sokolowski, and A. Collins, "Probabilistic risk analysis and terrorism risk," *Risk Analysis*, vol. 30, no. 4, pp. 575–589, Apr. 2010.

[19] National Research Council, *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change*. Washington, DC: The National Academies Press, 2008.

[20] National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*. Washington, DC: The National Academies Press, 2010.

[21] B. Cipiti, G. Wyss, F. Duran, and T. Lewis, "Security risk management of small modular reactors," Sandia National Laboratories, Albuquerque, NM, Tech. Rep., 2013.

[22] Westinghouse. (2013, Sep.) Columbia site. [Online]. Available: http://www.westinghousenuclear.com/ProductLines/Nuclear_Fuel/columbia_site.shtm

[23] Nuclear Regulatory Commission. (2013, Sep.) Transportation of spent nuclear fuel. [Online]. Available: http://www.nrc.gov/waste/spent-fuel-transp.html

[24] A. Parker, "A transparent success: 'Megatons to Megawatts' program," *Lawrence Livermore National Laboratory Science & Technology Review*, Apr./May 2013.

[25] World Nuclear Association. (2013, Sep.) Radioactive waste management: Managing HLW from used fuel. [Online]. Available: http://world-nuclear.org/info/Nuclear-Fuel-Cycle/Nuclear-Wastes/Radioactive-Waste-Management/#ManageHLW

[26] F. Harper, S. Musolino, and W. Wente, "Realistic radiological dispersal device hazard boundaries and ramifications for early consequence management decisions," *Health Physics*, vol. 93, no. 1, pp. 1–16, 2007.

[27] V. Reshetin, "Estimation of radioactivity levels associated with a ^{90}Sr dirty bomb event," *Atmospheric Environment*, vol. 39, no. 25, pp. 4471–4477, Aug. 2005.

[28] Center for International Earth Science Information Network (CIESIN)/Columbia University, United Nations Food and Agriculture Programme (FAO), and Centro Internacional de Agricultura Tropical (CIAT). (2005) Gridded Population of the World, Version 3 (GPWv3): Population Count Grid. NASA Socioeconomic Data and Applications Center (SEDAC). Palisades, NY. [Online]. Available: http://sedac.ciesin.columbia.edu/data/set/gpw-v3-population-count

[29] M. Scaparra and R. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Computers & Operations Research*, vol. 35, no. 6, pp. 1905–1923, 2008.

[30] G. Brown, M. Carlyle, A. Abdul-Ghaffar, and J. Kline, "A defender-attacker optimization of port radar surveillance," *Naval Research Logistics*, vol. 58, no. 3, pp. 223–235, 2011.

[31] D. Alderson, G. Brown, M. Carlyle, and K. Wood, "Solving defender-attacker-defender models for infrastructure defense," *Operations Research, Computing, and Homeland Defense*, pp. 28–49, 2011.

[32] T. Magnanti and R. Wong, "Network design and transportation planning: Models and algorithms," *Transportation Science*, vol. 18, no. 1, pp. 1–55, Feb. 1984.

[33] World Nuclear Association. (2013, Sep.) Nuclear fuel fabrication. [Online]. Available: http://world-nuclear.org/info/Nuclear-Fuel-Cycle/Conversion-Enrichment-and-Fabrication/Fuel-Fabrication

[34] Colorado Department of Transportation. (2013, Apr.) Colorado hazardous and nuclear materials routes restrictions 2013(a). [Online]. Available: http://dtdapps.coloradodot.info/staticdata/Downloads/StatewideMaps/HazMatMap.pdf

[35] M. Riddel, C. Dwyer, and W. Shaw, "Environmental risk and uncertainty: Insights from Yucca Mountain," *Journal of Regional Science*, vol. 43, no. 3, pp. 435–458, 2003.

Initial Distribution List

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California